ElGamal Encryption
과제

ElGamal Encryption

$(G, p, g) \leftarrow Gen(1^k)$

$x \leftarrow^{\$} Z_p, \quad y = g^x$

$PK = (G, p, g, y)$

$SK = x$

PK

CT

$Enc_{PK}(m)$:

$r \leftarrow^{\$} Z_p$

$CT = < g^r, m \cdot y^r >$

$Dec_{SK}(CT)$:

$C1, C2 \leftarrow CT$

$m = \frac{C2}{C1^x}$

Setup :

p ← random 1024 bit safe prime

g (p의 generator)

x ← Z_p

y = g^x mod p

pub = (p,g,y)

priv = x

Enc(m, pub) :

r ← Z_p

c_1 = g^r mod p

c_2 = m·y^r mod p

Dec(C, priv, pub) :

C = (c_1, c_2)

m = $\frac{c_2}{c_1^x}$ mod p <- c_2와 c_1^x의 inverse(mod p 에 대한) 를 곱하면 됩니다.

= c_2 * inv(c_1^x) mod p

출력 예:

```
Complete the select of safe prime
Complete the select of generator
p       : D5ED6D8C3A0192340D253236F3AB15C3472
D2D777AD16ADD4C768C5962C782A5415D064B07FD2F8A
g       : 05
c1      : A184EEDDB9C59F6AD1E968F81C39D63D001
8AC96E2F337F559AB2A3C13FE3607A9F3B76261D403F8
c2      : 56DD982EC04F4F51A29607BC948A49A3C91
6A6894DB4E58F686561353D70C972DB03490ED1779E63
dec     : hello
msg_len : 5
```

※실행이 수 초간 소요될 수 있음